TCCR Teleconference 7/17/02

Attendance

Bob Kohler (Chair), Craig Joyner, Annie Thomson, Don Mock, Jeremy Warren, Jeff Horn, Glen Muhr, Ron Bewtra, Russ Richards, Kirk Thoning, Alex Hsii, John Parker, Rich Beeler, Chris Cornwall, Gary Skaggs, James Abetya, Walt Harrop, Joan Brundage, John Hernandez

Recommendations

Official TCCR response to the latest security incidents:

The TCCR will form a subcommittee to come up with a broad security approach for all of OAR. This subcommittee will:

- Include members of the TCCR and lab ITSO's to gather the best expertise in OAR on the subject.
- Be given all of the incident reports submitted over the last year to pinpoint OAR's largest vulnerabilities.
- Document formal recommendations for mitigating OAR's IT security vulnerabilities.

Bob Kohler will form the subcommittee and set an initial meeting date for the first or second week of August.

Meeting Minutes

Security problem – What is the professional opinion of the TCCR on how to cut down the OAR hacks?

Three suggestions from Diane Davadiwizc

1. Firewall
2. Patch Management
3. Disable unneeded services

CMDL Hack

Diane – May have been exploited a sshd vulnerability on linux

Kirk – Web server hit, may be an apache vulnerability before the patch was out

- N-CIRT doesn't exactly know how they got in yet
- May be a CGI bin script problem
- Attacked other systems in CMDL from there
- Scanned all 140.90.x.x systems

ARL Hack

- Chris Cornwall wasn't informed of the ARL FTP hack
- No real details for the TCCR

- Located outside the firewall

Good to have TCCR de-brief on these security incidents

Don's Report on HQ

- HQ reaction was originally to force everyone to get a firewall
- OAR gets more hacks than other LO's => HQ needs to feel like it's taking action
- Don requested 24 hours to consult the TCCR
- OAR is particularly vulnerable because of lot of systems outside the firewalls for collaboration purposes
- What's the definition of a Firewall – Define (Russ)
- Would like to implement one, but there's a resource issue and wouldn't like it to be done the way NMFS did there's (Russ)
- Russ would like more specific instructions for what needs to be done (stateful configuration)

- The Problem is that OAR gets hacked a disproportional amount compared to the rest of NOAA
- We could solve this problem by not reporting attacks (Chris)
- Ron Bewtra suggested using an industry standard definition for a firewall and requiring that (recommended O'Reilly book)

- Don's Business Case
  - OAR is experiencing an inordinate about of downtime which disrupts business
  - Files could be changed or deleted and seriously impact productivity
- Walt suggested generally distributing trip wires and other tools, not just firewalls
- CMDL had filtering on their router, only port 80 was open to the outside so a firewall wouldn't have mattered (Kirk)
  - A proxy might have helped though (inbound and outbound)
- Anyone that doesn't have a firewall at all?
  - CDC doesn't (in progress)
  - Depends on the definition
  - Others?
- Is it reasonable to tell Dave that we're doing enough now with the three levels of the security? (Rich)
- Poorly setup and managed firewalls can do more harm than good (John Parker). Can lead to a false sense of confidence (Walt)
- The more services and platforms we have, the greater the chance that we'll have security problems (John Hernandez)

- HQ might want to emphasis to Lab Directors that we need to have more staff on security in the field (Russ)

- Diversity can work to our advantage – one hack doesn't take us all down (Chris)
- Nothing could stop the CMDL hack except extreme vigilance, but that requires more resources (i.e. people).
- AL as a full time security person
- CDC has a half time person
- AOML has part of a Unix SA's time

- First step in Boulder is Network Infrastructure, then they'll look at implementing security
- Security is very challenging because of high bandwidth connections

- Solution – Have TCCR study the overall problem
    - This would allow management to take action and allow the labs to look into real solutions
    - Labs should be sharing incident information between offices (like CMDL did with this last incident)
    - Limited resources (labor and money) means that it will take time
    - HQ should emphasis importance of security activities to the Lab Directors
    - Each lab should make it clear to HQ how exactly they've been shifting resources to account for increase security concerns
    - Bulleted list of baseline for each lab
    - Form a subcommittee
    - Share information between labs
    - Include not just TCCR members but also ITSO's => get the best expertise
    - Start out with a meeting at the Boulder Expo with Bob Kohler, Gary Skaggs, John Parker
    - Goal: Come up with a document saying what OAR should do for security on all levels; Short and Long term

- It would be nice to have an Architecture type document that is actually useful
    - Practical advise
    - Not bureaucratic
    - Short and Simple
- Arbitrarily mandating firewalls doesn't address the real problems and will take a lot of resources to implement